Remarks:

Status of the Claims

In the office action of April 4, 2010, Claims 1, 2, 4-6, 8 and 9 stand rejected.

Claims 1, 6 and 8 are amended herein. Claims 10 – 12 are added herein. Claims 1-2 and 4 – 6, and 8 – 12 are now pending in the application.

The Claims

35 USC 103

Claims 1, 2, 4-6, 8 and 9 stand rejected under 35 USC 103(a) as being unpatentable over Lim (U.S. Pat. Pub. 2002/0003876 A1, "Lim") in view of Sibert (U.S. Pat. No. 6,832,316 B1, "Sibert") as evidenced by Hein, James L. "Discrete Mathematics." ("Hein").

Applicants have amended the independent claims. To the extent the Examiner believes the rejection applies to the amended claims, Applicants traverse the rejection.

Applicants' novel and non-obvious technology comprises two parts, namely, a mapping of a cipher function f(x) to another function, a *super-function*, f' that may be performed instead of f(x) and a verification function. In the Office Action of April 7, 2009, the Examiner looked to Lim for the first of these parts and to Siebert, for the second.

Claim 1 recites a method that obtains the results of a cryptography process without performing one of the calculations normally present in that cryptography process. To avoid performing that calculation, the method includes the following step:

"performing a modified calculation in lieu of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a

function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' in a set F, wherein x is a member of E and f(x) is a member of the set F." (emphasis added).

In DES cryptography, *elementary operation* refers to several specific operations of the algorithm. Consider, for example, Lu, Jiquiang, et al. *Principles on the Security of AES against First and Second-Order Differential Power Analysis, in Applied Cryptography and Network Security: 8th International Conference, ACNS 2010 (Proceedings)*, (Jianying Zhou and Moti Yung (Eds.), page 171 (reproduced herein as Exhibit A). Zhou et al. states that the AES cipher (AES is a version of DES) uses four elementary operations: AddRoundKey, SubBytes, ShiftRows, and MixColumns.

The Examiner pointed to Lim, Figure 1, elt. CIPHER FUNCTION, for the teaching of the elementary operation f(x). Lim's CIPHER FUNCTION comprises four operations illustrated in Figure 1, namely: the expansion permutation 110, the XOR operation 120, the S-box 130, and the P-Box 140. In the vernacular of cryptography, these operations are elementary operations. The CIPHER function itself, being made up of several elementary operations, cannot be considered an *elementary operation*.

Thus, the calculation in Lim of the CIPHER function using the operations 110, 130, and 140 cannot be considered calculating the result of an elementary operation without performing that elementary operation by using a super-function.

The Examiner makes the statement in the office action that "[if] the prior art structure is capable of performing the intended use, then it meets the claim." Office Action, Page 3, Numbered Paragraph 4. That may be correct. However, if the intended use is to avoid differential fault analysis attacks by avoiding performing an elementary operation, there is nothing

in Lim that suggests a structure for achieving that result. Each of the elementary operations, e.g., 110, 130, and 140, that make up the CIPHER FUNCTION of Lim are performed in Lim. Thus, a differential fault analysis attack could be targeted at one or more of those operations. Lim does not teach or suggest a mechanism for avoiding such an attack.

New Claims 10, 11, and 12 add the limitation that "the elementary operation f(x) is a substitution function of a DES cryptography algorithm." As the CIPHER FUNCTION of Lim includes at least three other operations, it cannot be considered to meet this limitation. Furthermore, reading the added limitation into Claims 1, 6, and 8, respectively, illustrate that the elements 110, 130, and 140 of Lim cannot be used to meet the limitation of "performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F."

Applicants invite the Examiner to reconsider the arguments made in the previous office action response (15 March 2010) in light of the above explanation of the meaning of *elementary operation* in the context of DES cryptography. Those arguments are incorporated herein by reference with the extension in the form of the above-provided definition of *elementary operation.*

For the reasons provided in the previous office action response in light of the above explanation of *elementary operation*, Claim 1 is patentable over Lim.

The Examiner turns to Sibert for teaching of the verification function. This is an incorrect reading of Sibert. Applicants claim "operating the processor of the electronic assembly according to

instructions stored in the storage means to perform the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature." Sibert, in contrast, teaches in Figures 1A and 1B, cited by the Examiner, teaches "the sender generates the message authentication code (MAC) 16 by applying MAC function 18 to plaintext 10" (Sibert, Col. 1, Line 66 – Col. 2, Line 1, and "decryption function 20 yields a plaintext representation of the message 22, which the recipient checks for authenticity by computing a MAC 24. MAC 24 is compared to MAC 16' (i.e., the received version of MAC 16)" (Col. 2, Lines 5 – 10). Thus, Sibert teaches performing the verification by computing a MAC on the input and output of the encryption and decryption operations, respectively, rather than on an intermediate calculation as specified in Applicants claims.

It may be useful to consider the sequence of operations suggested by Applicants' claim. First the input x is mapped using the mapping $h1$. Next, the super-function f' is calculated using the mapping result. Finally, the output is produced by mapping the result from f' using the mapping $h2$. The verification operation is performed on the result of the super-function f'. Since Siebert teaches that the MAC operations is performed on the Plaintext input message and the Plaintext' output message, Siebert's validation operations cannot be considered being performed on the result obtained by the super function as claimed.

Accordingly, Siebert fails to teach or suggest "operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function using the result obtained by the super function in order to obtain a calculation signature."

Sibert like Lim fails to teach or suggest mapping input and output such that a super-function (as defined in this application) may be used as

a substitute for performing an elementary operation of a calculation to be secured. Therefore, Sibert fails to make up the deficiencies of Lim.

Accordingly, Claim 1 is patentable over Lim and Sibert taken singly or in combination.

Claims 6 and 8 recite analogous limitations to the limitations argued in support of Claim 1. These claims are patentable over the combination of Lim and Sibert for, at least, the reasons given in support of Claim 1.

Claims 2, 4, 5, 9, and 10 depend from Claim 1, Claims 11 and 12, depend from Claims 6 and 8, respectively. These dependent claims inherit the limitations of their respective base claims, provide further unique and non-obvious combinations, and are patentable for the reasons given in support of the independent claims and by virtue of such further combinations.

For the foregoing reasons, the combination of Lim and Sibert taken singly or in combination does not result in Applicants' claimed invention.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: July 12, 2010

/Pehr Jansson/
Pehr Jansson

Registration No. 35,759

The Jansson Firm
3616 Far West Blvd #117-314
Austin, TX 78731
512-372-8440
512-597-0639 (Fax)
pehr@thejanssonfirm.com